FIG.1

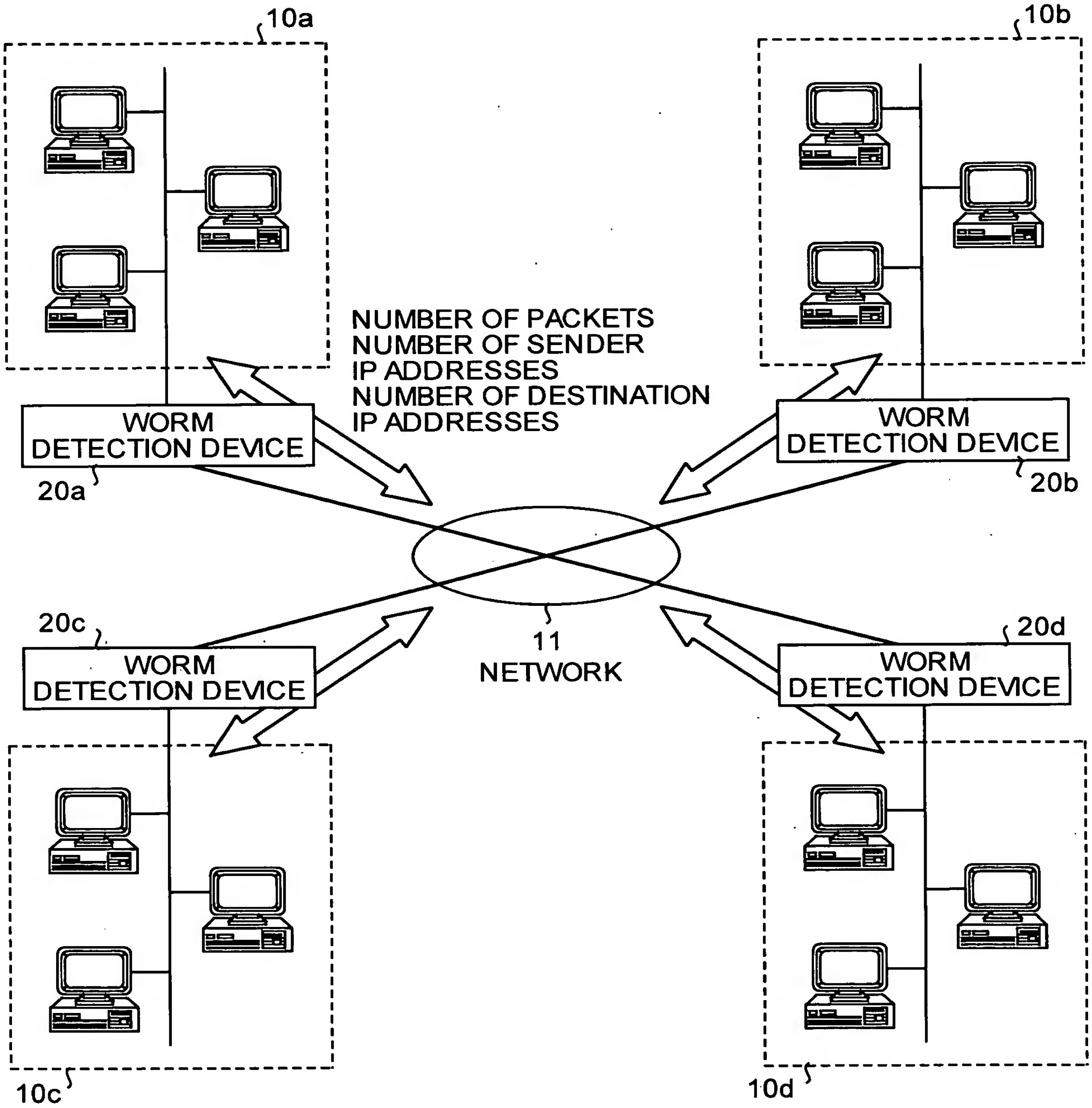

10a
10b
NUMBER OF PACKETS
NUMBER OF SENDER
IP ADDRESSES
NUMBER OF DESTINATION
IP ADDRESSES
WORM
DETECTION DEVICE
20a
WORM
DETECTION DEVICE
20b
20c
WORM
DETECTION DEVICE
11
NETWORK
20d
WORM
DETECTION DEVICE
10c
10d

FIG.2

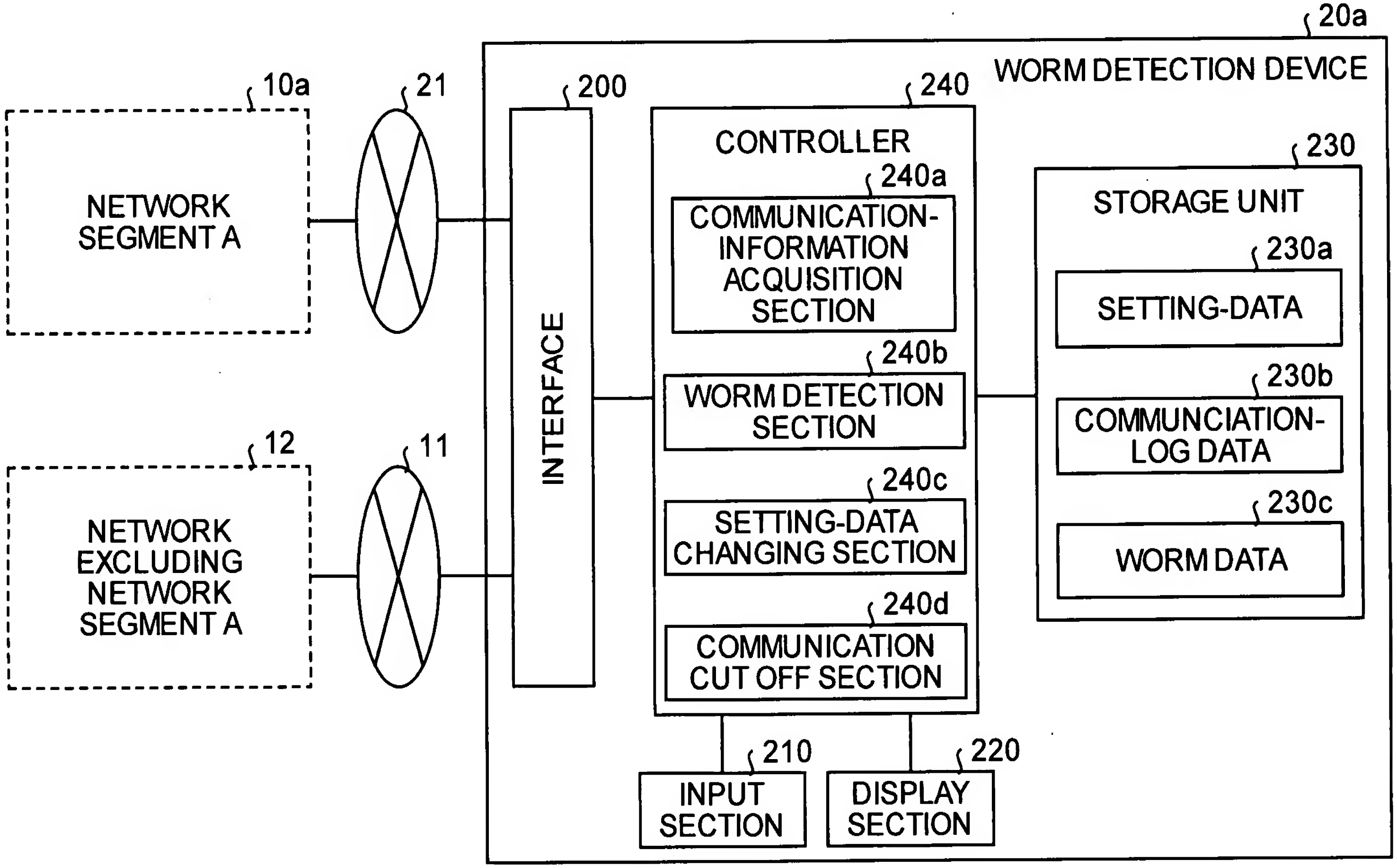

20a
WORM DETECTION DEVICE
10a
NETWORK SEGMENT A
21
12
NETWORK EXCLUDING NETWORK SEGMENT A
11
200
INTERFACE
240
CONTROLLER
240a
COMMUNICATION-INFORMATION ACQUISITION SECTION
240b
WORM DETECTION SECTION
240c
SETTING-DATA CHANGING SECTION
240d
COMMUNICATION CUT OFF SECTION
230
STORAGE UNIT
230a
SETTING-DATA
230b
COMMUNCIATION-LOG DATA
230c
WORM DATA
210
INPUT SECTION
220
DISPLAY SECTION

FIG.3

SETTING-DATA 230a

SETTING ITEMS	INITIAL SETTING	SETTING AFTER DETECTION OF FAULT IN SYN PACKET
UNIT TIME FOR MEASUREMENT OF NUMBER OF SYN PACKETS	1 sec	0.1 sec
UNIT TIME FOR MEASUREMENT OF NUMBER OF SYN ACK PACKETS	1 sec	1 sec
UNIT TIME FOR MEASUREMENT OF NUMBER OF UDP PACKETS	1 sec	1 sec
UNIT TIME FOR MEASUREMENT OF NUMBER OF ICMP (request) PACKETS	1 sec	1 sec
UNIT TIME FOR MEASUREMENT OF NUMBER OF ICMP (response) PACKETS	1 sec	1 sec
UNIT TIME FOR MEASUREMENT OF NUMBER OF DESTINATION IP ADDRESSES	1 sec	0.1 sec
UNIT TIME FOR MEASUREMENT OF NUMBER OF SENDER IP ADDRESSES	1 sec	1 sec
REFERENCE OF DESTINATION PORT NUMBER	OFF	ON
THRESHOLD VALUE OF NUMBER OF SYN PACKETS	10	2
THRESHOLD VALUE OF NUMBER OF SYN ACK PACKETS	10	10
THRESHOLD VALUE OF NUMBER OF UDP PACKETS	10	10
THRESHOLD VALUE OF NUMBER OF ICMP (request) PACKETS	10	10
THRESHOLD VALUE OF NUMBER OF ICMP (response) PACKETS	10	10
THRESHOLD VALUE OF NUMBER OF DESTINATION IP ADDRESSES	10	2
THRESHOLD VALUE OF NUMBER OF SENDER IP ADDRESSES	10	10
MONITORING LOCATION	Eth0	Eth0
DIRECTION OF NETWORK TO BE MONITORED	Outgoing	Outgoing
CUT OFF	OFF	ON
TIME FROM DETECTION TO CUT OFF	5 sec	5 sec

FIG.4

COMMUNICATION-LOG DATA
230b

MEASUREMENT TIME	NUMBER OF PACKETS					NUMBER OF IP ADDRESSES	
	NUMBER OF SYN PACKETS	NUMBER OF SYN ACK PACKETS	NUMBER OF UDP PACKETS	NUMBER OF ICMP (request) PACKETS	NUMBER OF ICMP (response) PACKETS	NUMBER OF DESTINATION IP ADDRESSES	NUMBER OF SENDER IP ADDRESSES
10:00:34 TO 10:00:35	4	4	7	0	0	8	9
10:00:35 TO 10:00:36	5	30	4	1	1	7	36
10:00:36 TO 10:00:37	5	5	4	2	2	6	8
10:00:37 TO 10:00:38	22	4	7	0	0	28	8
10:00:38 TO 10:00:39	4	4	7	0	0	10	9
10:00:39 TO 10:00:40	49	5	8	0	0	60	10
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

FIG.5

CASE NUMBER	STATUS	JUDGMENT	PROCESS
1	INCREASE IN NUMBER OF SYN PACKETS AS WELL AS OF DESTINATION IP ADDRESSES IN Outgoing COMMUNICATION	TCP-BASED WORM	DETECTION OF AS TO WHICH SERVICE ATTACKING WORM IT IS FROM MOST FREQUENTLY TARGETTED PORT NUMBER. PORT NUMBER 80: Web SERVICE
2	INCREASE IN NUMBER OF UPD PACKETS AS WELL AS OF DESTINATION IP ADDRESSES IN Outgoing COMMUNICATION	UDP-BASED WARM	DETECTION OF AS TO WHICH SERVICE ATTACKING WORM IT IS FROM MOST FREQUENTLY TARGETTED PORT NUMBER. PORT NUMBR 53: DNS SERVICE
3	INCREASE IN NUMBER OF ICMP (request) PACKETS AS WELL AS OF DESTINATION IP ADDRESSES IN Outgoing COMMUNICATION	—	MONITORING OF SUBSEQUENT SYN PACKETS OR UDP PACKETS, JUDGING WHETHER IT IS TCP BASED WORM OR UDP BASED WORM, AND DETECTION OF AS TO WHICH SERVICE ATTACKING WORM IT IS FROM MOST FREQUENTLY TARGETTED PORT NUMBER

FIG.6

COMMUNICATION-LOG DATA 230b

MEASUREMENT TIME	NUMBER OF PACKETS	NUMBER OF IP ADDRESSES
	NUMBER OF SYN ACK PACKETS	NUMBER OF SENDER IP ADDRESSES
10:00:35 TO 10:00:36	30	36
MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER	80(90%)	80(92%)

WORM DETECTION RESULT 60

WORM DETECTION RESULT
→SCAN METHOD: SYN PACKET
→SCAN ORIGIN IP ADDRESS: 192.10.1.14
→MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER: 80

THERE IS A POSSIBILITY OF INVASION FROM OUTSIDE BY WORM THAT TARGETS VULNERABILITY OF Web SERVICE.

FIG.7

COMMUNICATION-LOG DATA
230b

MEASUREMENT TIME	NUMBER OF PACKETS	NUMBER OF IP ADDRESSES
	NUMBER OF SYN PACKETS	NUMBER OF DESTINATION IP ADDRESSES
10:00:37 TO 10:00:38	22	28
MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER	80(94%)	80(89%)

WORM DETECTION RESULT
70

WORM DETECTION RESULT
→SCAN METHOD: SYN PACKET
→SCAN RATE: 10 scan/sec
→NUMBER OF COMPUTERS INFECTED: 1
→NAME OF COMPUTER INFECTED: lemon
→IP ADDRESS OF COMPUTER INFECTED: 192.10.3.5
→MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER: 80

- Web SERVER INSIDE SEGMENT MAY HAVE BEEN INFECTED.
- SCAN FEATURES RESEMBLE TO THOSE OF Blaster WORM.
- NETWORK 192.10.4.0/24 SCANNED

FIG.8

COMMUNICATION-LOG DATA 230b

MEASUREMENT TIME	NUMBER OF PACKETS		NUMBER OF IP ADDRESSES	
	NUMBER OF SYN PACKETS	NUMBER OF SYN ACK PACKETS	NUMBER OF DESTINATION IP ADDRESSES	NUMBER OF SENDER IP ADDRESSES
10:00:35 TO 10:00:36	5	30	7	36
10:00:36 TO 10:00:37	5	5	6	8
10:00:37 TO 10:00:38	22	4	28	8
MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER	80(87%)	80(87%)	80(89%)	80(86%)

⇩

WORM DETECTION RESULT 80

WORM DETECTION RESULT
→SCAN METHOD : SYN PACKET
→MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER : 80

Web SERVER INSIDE SEGMENT MAY HAVE BEEN INFECTED.

FIG.9

COMMUNICATION-LOG DATA
230b

MEASUREMENT TIME	NUMBER OF PACKETS	NUMBER OF IP ADDRESSES
	NUMBER OF SYN PACKETS	NUMBER OF DESTINATION IP ADDRESSES
10:00:37 TO 10:00:38	22	28
10:00:38 TO 10:00:39	4	10
10:00:39 TO 10:00:40	49	60
MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER	80(92%)	80(95%)

⇩

WORM DETECTION RESULT
90

WORM DETECTION RESULT
→SCAN METHOD: SYN PACKET
→SCAN RATE: 10 scan/sec
→NUMBER OF COMPUTERS INFECTED: 1→2
→NAME OF COMPUTER INFECTED: lemon,apple
→IP ADDRESS OF COMPUTER INFECTED: 192.10.2.5,192.10.2.11
→MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER: 80

Web SERVER INSIDE SEGMENT MAY HAVE BEEN INFECTED.

FIG.10

METHOD	PROCESS	REFERENCE INFORMATION
1	CUTTING OFF SPECIFIC Outgoing COMMUNICATION (RANDOM SCAN) FROM NETWORK SEGMENT INCLUDING COMPUTER INFECTED BY WORM	COMMUNICATION PROTOCOL (TCP/UDP) MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER
2	CUTTING OFF SPECIFIC Outgoing COMMUNICATION FROM COMPUTER INFECTED BY WORM	COMMUNICATION PROTOCOL (TCP/UDP) SENDER IP ADDRESS MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER
3	STOPPING RANDOM SCAN OF COMPUTER INFECTED BY WORM, BY REMOTE OPERATION AFTER PROCESS 1 OR 2 (STOPPING PROCESS OF RANDOM SCAN, CUTTING OFF RANDOM SCAN SUCH AS PERSONAL FIRE WALL ETC. IN DEVICE)	COMMUNICATION PROTOCOL (TCP/UDP) SENDER IP ADDRESS MOST FREQUENTLY TARGETTED DESTINATION PORT NUMBER

FIG.11

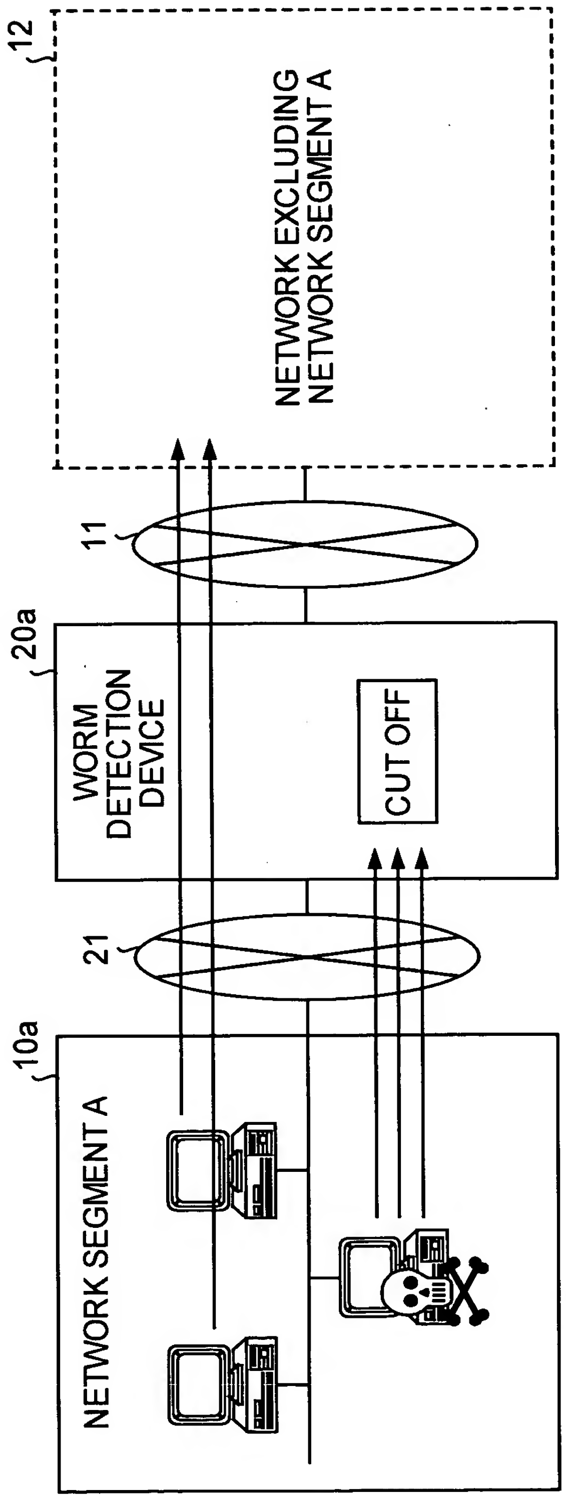

12
NETWORK EXCLUDING NETWORK SEGMENT A
11
20a
WORM DETECTION DEVICE
CUT OFF
21
10a
NETWORK SEGMENT A

FIG.12

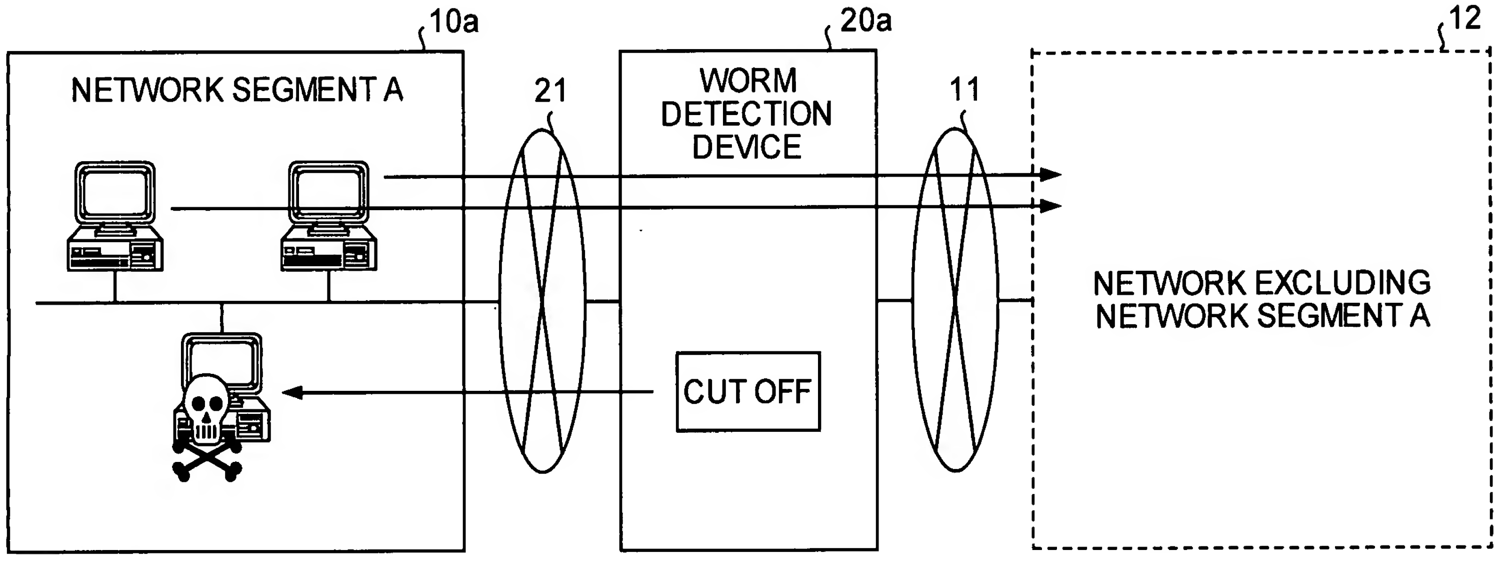

10a
NETWORK SEGMENT A
21
20a
WORM DETECTION DEVICE
CUT OFF
11
12
NETWORK EXCLUDING NETWORK SEGMENT A

FIG.13

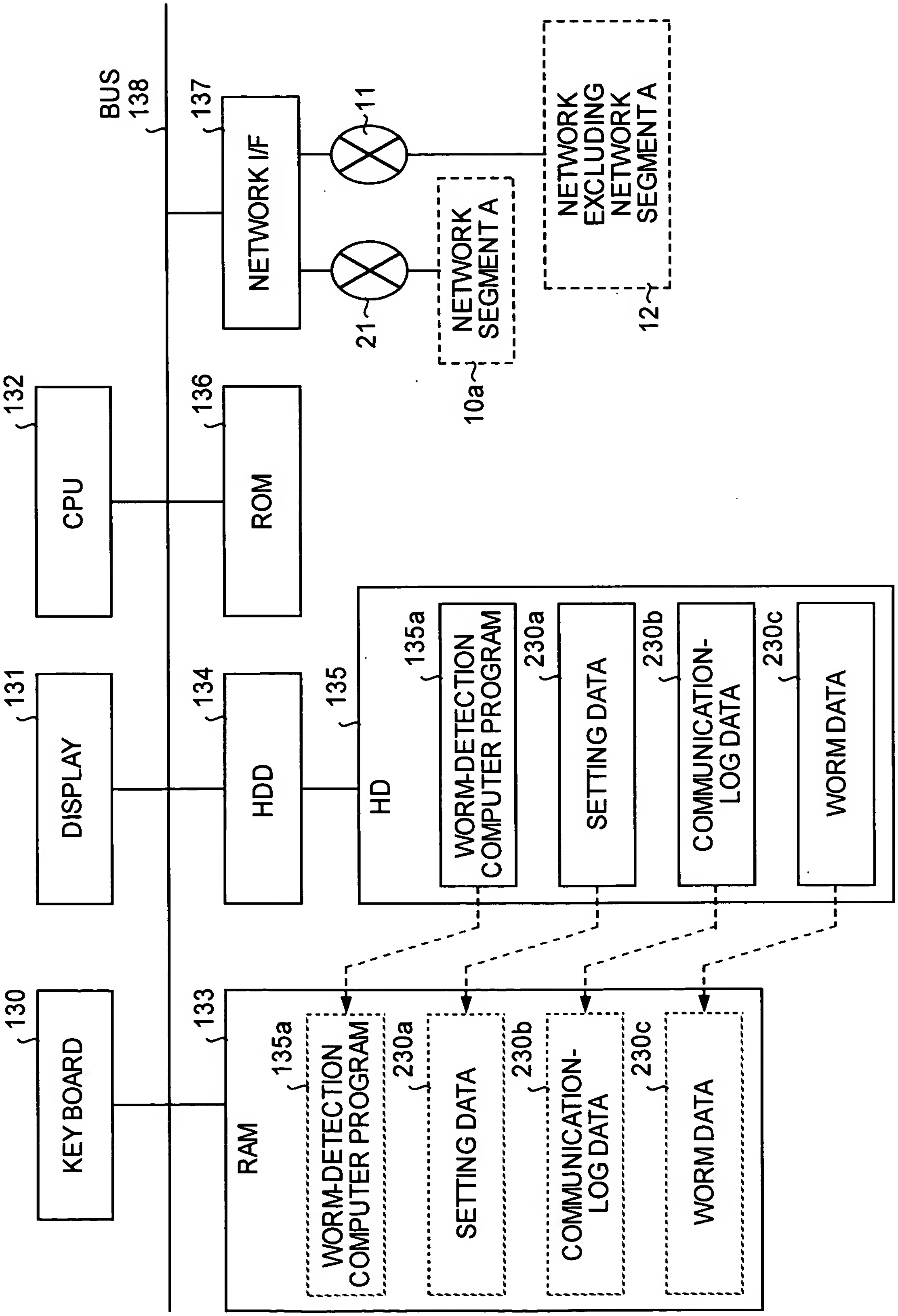

BUS
138
KEY BOARD
130
DISPLAY
131
CPU
132
RAM
133
HDD
134
ROM
136
NETWORK I/F
137
HD
135
WORM-DETECTION COMPUTER PROGRAM
135a
SETTING DATA
230a
COMMUNICATION-LOG DATA
230b
WORM DATA
230c
WORM-DETECTION COMPUTER PROGRAM
135a
SETTING DATA
230a
COMMUNICATION-LOG DATA
230b
WORM DATA
230c
21
11
NETWORK SEGMENT A
10a
NETWORK EXCLUDING NETWORK SEGMENT A
12

FIG.14

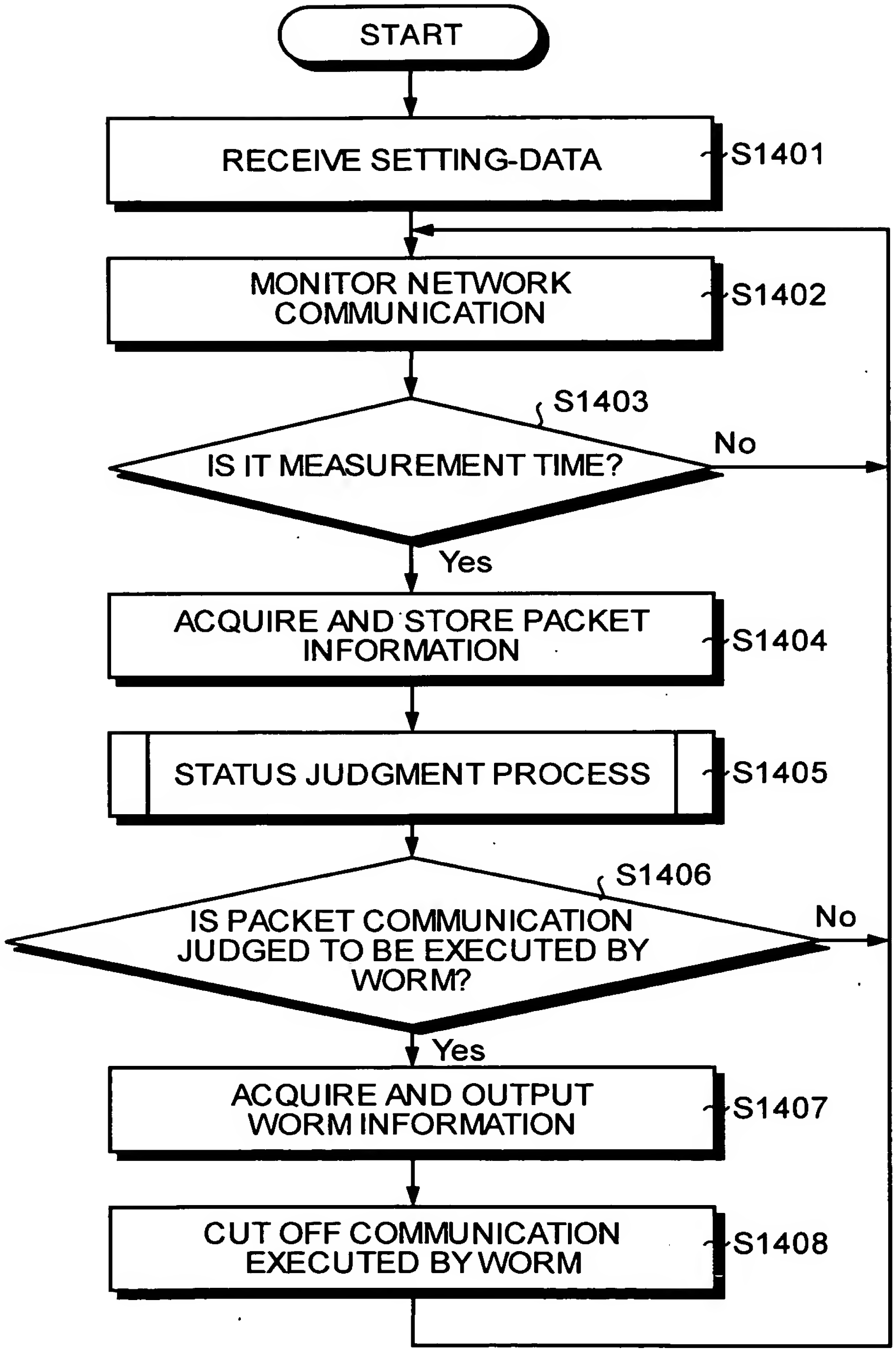

START
RECEIVE SETTING-DATA
S1401
MONITOR NETWORK COMMUNICATION
S1402
S1403
IS IT MEASUREMENT TIME?
No
Yes
ACQUIRE AND STORE PACKET INFORMATION
S1404
STATUS JUDGMENT PROCESS
S1405
S1406
IS PACKET COMMUNICATION JUDGED TO BE EXECUTED BY WORM?
No
Yes
ACQUIRE AND OUTPUT WORM INFORMATION
S1407
CUT OFF COMMUNICATION EXECUTED BY WORM
S1408

FIG.15A

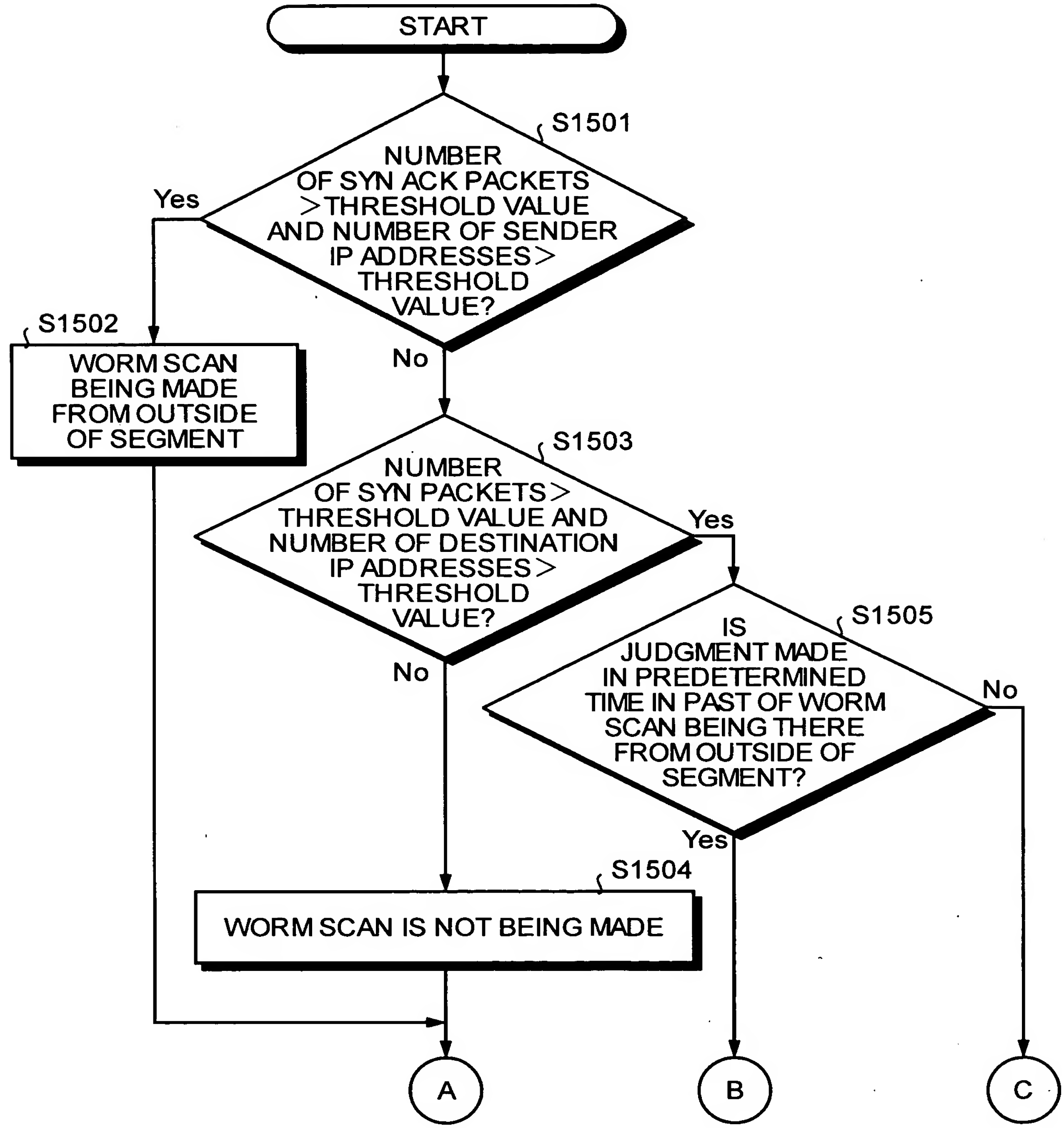
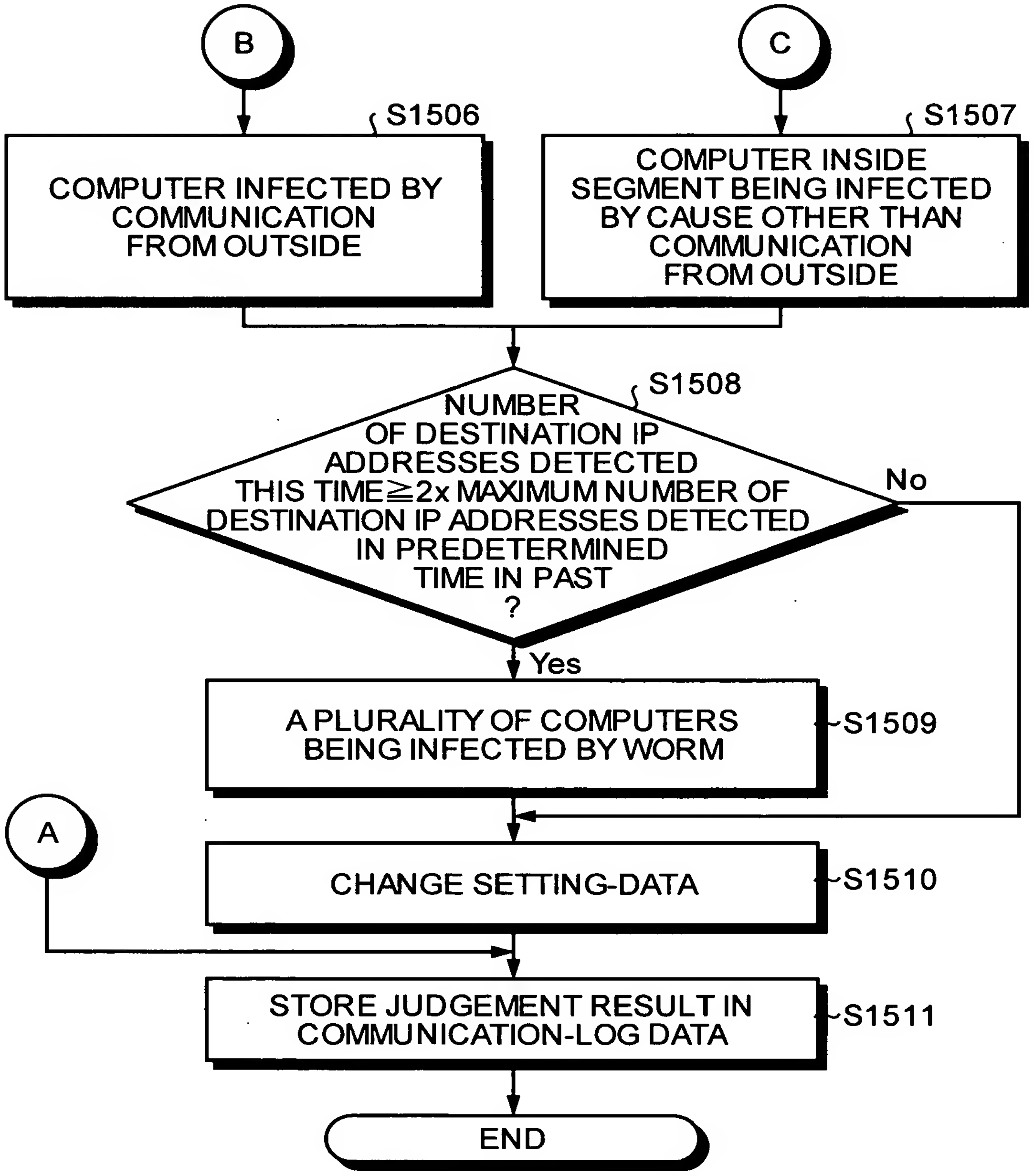
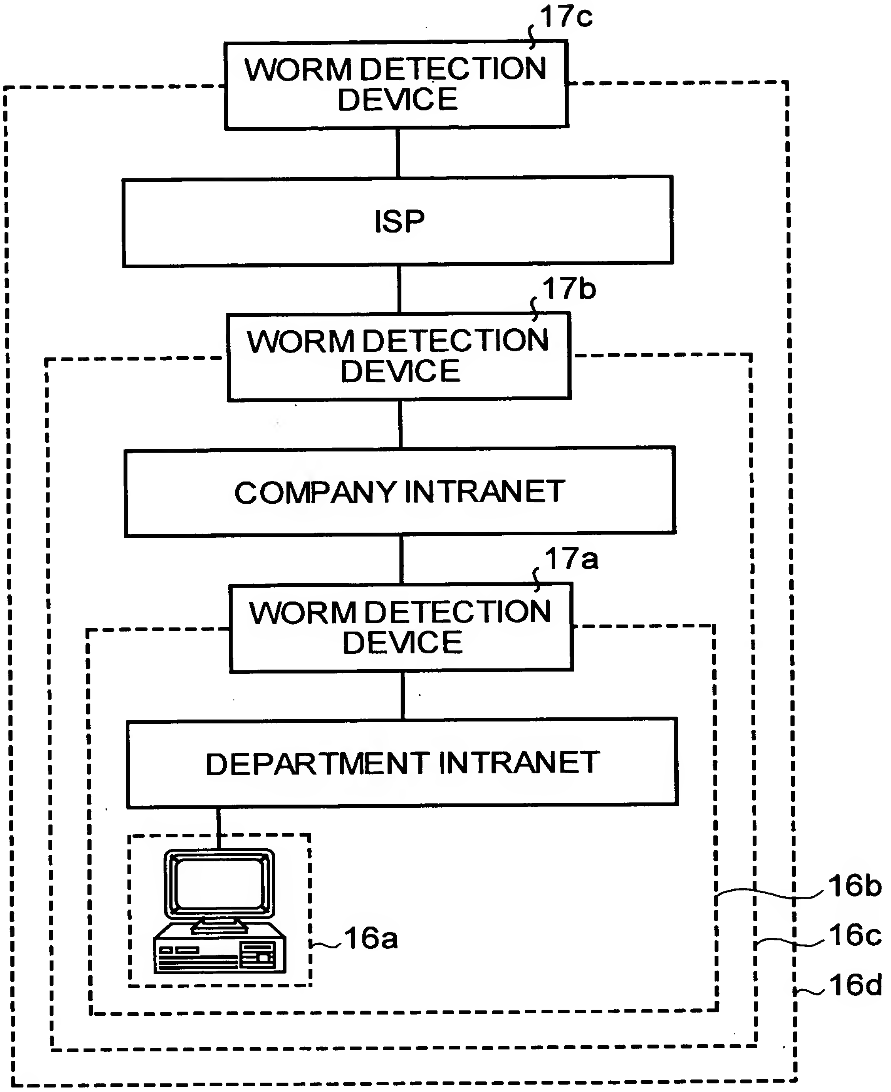

START
S1501
NUMBER OF SYN ACK PACKETS >THRESHOLD VALUE AND NUMBER OF SENDER IP ADDRESSES> THRESHOLD VALUE?
Yes
No
S1502
WORM SCAN BEING MADE FROM OUTSIDE OF SEGMENT
S1503
NUMBER OF SYN PACKETS> THRESHOLD VALUE AND NUMBER OF DESTINATION IP ADDRESSES> THRESHOLD VALUE?
Yes
No
S1505
IS JUDGMENT MADE IN PREDETERMINED TIME IN PAST OF WORM SCAN BEING THERE FROM OUTSIDE OF SEGMENT?
No
Yes
S1504
WORM SCAN IS NOT BEING MADE
A
B
C

FIG.15B


B
C
S1506
COMPUTER INFECTED BY COMMUNICATION FROM OUTSIDE
S1507
COMPUTER INSIDE SEGMENT BEING INFECTED BY CAUSE OTHER THAN COMMUNICATION FROM OUTSIDE
S1508
NUMBER OF DESTINATION IP ADDRESSES DETECTED THIS TIME≧2x MAXIMUM NUMBER OF DESTINATION IP ADDRESSES DETECTED IN PREDETERMINED TIME IN PAST ?
No
Yes
A PLURALITY OF COMPUTERS BEING INFECTED BY WORM
S1509
A
CHANGE SETTING-DATA
S1510
STORE JUDGEMENT RESULT IN COMMUNICATION-LOG DATA
S1511
END

DEVICE AND METHOD FOR WORM... March 30, 2004
Omote et al.
Greer, Burns & Crain, Ltd. (James K. Folker)
Ref. No. 1924.70199
Sheet 17 of 17 (312) 360 0080

FIG.16


17c
WORM DETECTION DEVICE
ISP
17b
WORM DETECTION DEVICE
COMPANY INTRANET
17a
WORM DETECTION DEVICE
DEPARTMENT INTRANET
16a
16b
16c
16d